REMARKS

This application has been carefully reviewed in light of the Office Action dated

December 3, 2003. Claims 1 to 26 remain pending in the application, of which Claims 1, 7, 13,

23, 24 and 26 are independent. Reconsideration and further examination are respectfully

requested.

Claims 1 to 26 were rejected under 35 U.S.C. § 103(a) over U.S. Patent No.

6,330,600 (Matchefts) in view of a Microsoft press release, "Universal Plug and Play ..."

(hereinafter referred to as "Microsoft") and further in view of U.S. Patent No. 6,009,103

(Woundy). Reconsideration and withdrawal of the rejections are respectfully requested.

The present invention concerns management of devices on a network,

according to the invention, a managing device receives a broadcast packet which is broadcast

from a device on the network at least once when the device is activated. The managing device

determines whether the received broadcast packet is a network managing packet, and if so,

acquires from the broadcast packet an address of the device that transmitted the packet. The

managing device then registers the acquired device address to, for example, an external apparatus

or a server. As a result, the network managing device simply listens for broadcast packets

broadcast by devices when they are activated so that real-time updates on the network devices

can be performed.

With specific reference to the claims, amended independent Claim 1 is a

network device managing apparatus for managing a network to which a device which broadcasts

a network managing packet at least once after activation is connected, comprising packet

receiving means for receiving a broadcast packet which is broadcast from the device when the

device is activated, packet determining means for determining whether the broadcast packet received by the packet receiving means is a network managing packet, device address acquiring means for acquiring from the broadcast packet an address of the device which has transmitted the broadcast packet, if the packet determining means determines that the broadcast packet is a network managing packet, and device address registering means for registering the device address acquired by the device address acquiring means.

Amended independent Claims 7 and 13 are system and method claims, respectively, that substantially correspond to Claim 1, and Claim 24 includes features similar to Claim 1, but includes the feature of registering the acquired address to an external managing apparatus.

Amended independent Claim 23 also includes features along the lines of Claim 1, but is more specifically directed to a network device managing apparatus for managing a network to which a device which broadcasts a network managing packet at least one after activation is connected, comprising a network interface circuit, and a trap monitor for (i) receiving, via the network interface circuit, a broadcast packet which is broadcast from the device when the device is activated, (ii) determining whether the broadcast packet received by the network interface circuit is a network managing packet, (iii) acquiring from the broadcast packet the address of the device which has transmitted the broadcast packet if it is determined that the broadcast packet is a network managing packet, and (iv) registering the acquired device address.

Amended independent Claim 26 is along the lines of Claim 23, but includes the feature of registering the acquired address to an external managing apparatus.

The applied art, alone or in any permissible combination, is not seen to disclose

- 11 -

or to suggest the features of Claims 1, 7, 13, 23, 24 and 26. More specifically, the applied art is not seen to disclose or to suggest at least the feature of a network managing device receiving a broadcast packet which is broadcast from a network device at least once when the device is activated, determining whether the broadcast packet is a network managing packet, if so, acquiring from the broadcast packet an address of the device which transmitted the broadcast packet, and registering the acquired device address.

The Office Action admits that Matchefts fails to disclose a device that broadcasts a packet when the device is activated, and acquiring an address of the device that transmitted the packet from the received packet, and registering the acquired address. Moreover, while Matchefts may receive a packet, the packet is not a broadcast packet that is broadcast by a network device at least once when the device is activated. Rather, Matchefts' packet is a TRAP packet that is provided to the managing apparatus by the device when a change is made in the configuration of the device. To accomplish this, since broadcasting is not used, the device transmitting the packet must know the address of the managing device in order for the device to provide the TRAP packet to the managing device. Accordingly, Matchefts operates in an entirely different manner than the present invention.

Microsoft is merely seen to disclose the use of Universal Plug and Play whereby, when a device is newly-installed, it automatically configures itself using TCP/IP and announces its presence on the network to other devices using the HTTP protocol. When one device wants to use the services of another device on the network, it sends out a discovery request to determine what devices on the network can meet the requested needs. Thus, a polling technique is used. Accordingly, although the newly-installed device may announce its presence

- 12 -

on the network, the device information is apparently not registered in any of the devices receiving such notification because the device wanting to use services of another device on the network has to perform the polling operation to find the devices that can perform the services rather than simply referring to a listing of registered devices. Therefore, any permissible combination of Matchefts and Microsoft would have, at best, resulted in new devices announcing their presence to the managing device of Matchefts, but would not have resulted in the managing device determining whether a broadcast packet is a network managing packet, and if so, acquiring from the broadcast packet an address of the device which transmitted the broadcast packet, and registering the acquired device address.

Woundy is merely seen to disclose a technique to register an IP address to an LDAP server by a DHCP server. According to the patent, the DHCP server assigns IP addresses to devices on the network when they are first activated. The assigned IP address is then registered in an LDAP server by the DHCP server so that other devices can use the services of the registered device. Thus, in Woundy, the DHCP server transmits the packet to the LDAP server and not the device being activated. Moreover, the LDAP server does not perform a determination as to whether or not the received packet is a managing packet, and if so, acquires an address of the device that sent the packet from the packet and registers the acquired address. That is, the LDAP server does not acquire the address of the DHCP server (the device which sent the packet) and register the address of the DHCP server, but rather, registers the address of the device for which the IP address was assigned by the DHCP server. Accordingly, Woundy is not seen to add anything that, when combined with Matchefts and Microsoft, would have rendered the present invention obvious.

In view of the foregoing amendments and remarks, the entire application is believed to be in condition for allowance and such action is respectfully requested at the Examiner's earliest convenience.

Applicant's undersigned attorney may be reached in our Costa Mesa, California office at (714) 540-8700. All correspondence should continue to be directed to our below-listed address.

Respectfully submitted,

Attorney for Applicant
Registration No. 42,746

FITZPATRICK, CELLA, HARPER & SCINTO
30 Rockefeller Plaza
New York, New York 10112-2200
Facsimile: (212) 218-2200

CA_MAIN 78050 v 1

- 14 -

ß